UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/900,493	07/06/2001	Michael Freed	NEXSI-01111US0	4137

28863 7590 03/23/2006

SHUMAKER & SIEFFERT, P. A.
8425 SEASONS PARKWAY
SUITE 105
ST. PAUL, MN 55125

EXAMINER	
LAFORGIA, CHRISTIAN A	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 03/23/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/900,493	FREED ET AL.	
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 December 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4-9 and 12-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4-9 and 12-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06 July 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *10/17/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 30 December 2005 has been entered.

2. Claims 1, 2, 4-9, and 12-20 have been presented for examination.

Response to Arguments

3. Applicant's arguments with respect to claims 1, 2, 4-9, 12-20 have been considered but are moot in view of the new ground(s) of rejection.

4. See further rejections that follow.

Specification

5. The use of the trademark Netscape has been noted in this application. It should be capitalized wherever it appears and be accompanied by the generic terminology.

6. Although the use of trademarks is permissible in patent applications, the proprietary nature of the marks should be respected and every effort made to prevent their use in any manner which might adversely affect their validity as trademarks.

Drawings

7. Figures 1, 2A, and 2B should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). Corrected drawings in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the

application. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections

8. Claims 1, 2, 4, 5, 7-9, 12, 13, and 16-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,681,327 to Jardin, hereinafter Jardin, in view of U.S. Patent No. 5,841,873 to Lockhart et al., hereinafter Lockhart.

9. As per claims 1, Jardin discloses a method for enabling secure communication between a client on an open network and a server apparatus on a secure network (Figure 1 [block 100]), the method performed on a intermediary apparatus coupled to the secure network and the open network (Figure 1 [block 120]), comprising:

negotiating a secure communications session with the client apparatus via the open network (Figure 2 [blocks 210, 220, 230, 240], describes the "handshake" between the client and the server which used to start any communication between the server and the client);

negotiating an open communications session with the server via the secure network (column 6, lines 40-46);

receiving encrypted packet application data for a security record spanning multiple data packets, wherein the security record has a length greater than a packet length associated with the multiple data packet (column 6, lines 65-69)

decrypting the encrypted packet application data in each data packet (column 6, line

67);

forwarding decrypted, unauthenticated application data to the server via the secure network (column 7, line 4).

10. Jardin doesn't teach discarding at least a portion of the decrypted unauthenticated packet application data for the security record prior to receiving a final packet of the security record and authenticating the data.

11. Lockhart discloses discarding at least a portion of the decrypted unauthenticated packet application data for the security record prior to receiving a final packet of the security record and authenticating the data (column 5, lines 33-65).

12. It would have been obvious to one ordinary skilled in the art at the time the invention was made to discard at least a portion of the decrypted unauthenticated packet application data for the security record prior to receiving a final packet of the security record and authenticating the data, since Lockhart states at column 5, lines 47-65 that such a modification would detect decryption errors in an encrypted data packet, thereby detecting if the packet may have been tampered with.

13. Regarding claim 2, Jardin system discloses forwarding data which spans over multiple TCP segments (column 7, lines 44-45).

14. Regarding claims 4 and 12, Jardin system discloses wherein a remaining portion of the packet application data for the security record is buffered as a minimal length sufficient to complete a block cipher used to encrypt the data (column 2, lines 65 to column 3, line 3). This

has been known in the art for quite some time and is support by U.S. Patent Nos. 6,101,543 (column 10, lines 58-67) and 5,825,890 (column 17, lines 21-40).

15. Regarding claims 5 and 19, Jardin discloses the use of TCP/IP. The Examiner holds that authenticating could only take place once the final segment was received, if it were fragmented since **Internetworking with TCP/IP**, by Douglas Comer (hereinafter Comer), states that if any fragments are missing the datagram cannot be reassembled on page 105.

16 As per claim 7, Jardin discloses a method for processing encrypted data transferred between a first system and a second system, comprising:

providing an accelerator device including a decryption engine in communication with the first system via an open network and the second system via a secure network (Figure 1 [block 120])

receiving encrypted data from the first system via the open network in the form of application data spanning multiple packets, wherein a last packet of the multiple packets includes information for authenticating the application data (column 6, line 67);

decrypting the application data contained within the multiple packets as the multiple packets are received (column 7, lines 39-41);

forwarding the decrypted application data as the multiple packets are decrypted to the second device via the secure network (column 7, line 4);

authenticating the application data when the information for authenticating the application data is received in the last of the multiple packets.

17. Jardin does not disclose buffering a portion of the decrypted application data and discarding a remaining portion prior to authentication of the application data.

18. Lockhart discloses buffering a portion of the decrypted application data and discarding a remaining portion prior to authentication of the application data (column 3, line 64 to column 4, line 17, column 5, lines 33-65).

19. It would have been obvious to one ordinary skilled in the art at the time the invention was made to discard at least a portion of the decrypted unauthenticated packet application data for the security record prior to receiving a final packet of the security record and authenticating the data, since Lockhart states at column 5, lines 47-65 that such a modification would detect decryption errors in an encrypted data packet, thereby detecting if the packet may have been tampered with.

20. Regarding claim 8, Jardin system teaches wherein receiving comprises receiving SSL encrypted data (column 4, lines 11-12).

21. Regarding claims 9, 13, 17, and 18, Jardin system teaches application data encrypted using SSL, DES, and a 3DES algorithm (column 5, lines 16-20).

22 As per claim 16, Jardin teaches a method of providing secure communications using limited buffer memory in a processing device (column 6, lines 5-11), comprising:

receiving encrypted data having a length greater than a TCP segment carrying said data (column 6, line 67);

the buffer having a length equivalent to the block cipher size necessary to perform the cipher (column 6, lines 9-14);

decrypting the buffered segment of the received encrypted data to provide decrypted application data (column 7, lines 39-41);

forwarding the decrypted application data to a destination device (column 7, lines 4).

23. Jardin does not disclose buffering.

24. Lockhart discloses the use of a buffer (column 3, line 64 to column 4, line 17,).

25. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use a buffer with an equivalent length to that necessary to perform a block cipher, since it has been held in the art (as illustrated by U.S. Patent Nos. 6,101,543 (column 10, lines 58-67) and 5,825,890 (column 17, lines 21-40) including additional data to a block cipher to make it the appropriate length improves the strength of the cipher.

26. Claims 6, 14, 15, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jardin in view of Lockhart as applied above, and further in view of U.S. Patent No. 6,052,785 to Lin et al., hereinafter Lin.

27. Regarding claims 6, 14, 15, and 20, Jardin and Lockhart do not teach after forwarding the decrypted unauthenticated application data to the server, notifying the client apparatus if a failure in authenticating the security record occurs.

28. Lin discloses after forwarding the decrypted unauthenticated application data to the server, notifying the client apparatus if a failure in authenticating the security record occurs (Figure 4 [blocks 418, 420], column 7, lines 25-41).

29. It would have been obvious to one of ordinary skill in the art at the time the invention was made to notify the client of a failure to authenticate, since Lin states at column 7, lines 19-24 that such a modification would allow a client to re-authenticate if their previous session and credentials had expired.

Conclusion

30. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

31. The following patents are cited to further show the state of the art with respect to SSL, such as:

United States Patent No. 6,993,651 to Wray et al., which is cited to show a security protocol through an intermediary device.

United States Patent No. 6,952,768 to Wray, which is cited to show a security protocol through an intermediary device.

32. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

33. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

34. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christian LaForgia
Patent Examiner
Art Unit 2131
clf

CHRISTOPHER REVAK
PRIMARY EXAMINER
CLL 3/17/06